THE AMERICAN MATHEMATICAL MONTHLY.

Entered at the Post-office at Springfield, Missouri, as Second-class Mail Matter.

VOL. VI. NOVEMBER, 1889. No. 11.

SOME ELEMENTS OF SUBSTITUTION GROUPS.

By DR. G. A. MILLER, Cornell University.

INTRODUCTORY NOTE. It is very gratifying to notice that the number of young men who desire to study modern mathematics is rapidly increasing. The best way to get a start in this direction is to attend some university where there are mathematicians who keep up with the rapid progress that is being made in different lines. While the summer sessions at the universities bring this method within the reach of a large class yet there are many who feel unable to pursue this course. These are frequently discouraged by the difficulties which they meet when they attempt to study the available treatises. The effort which this Journal is making to remove some of these difficulties seems to me to be very commendable. At the request of the editor I shall attempt to state some of the elements of substitution groups in a very simple manner, since it appears that I proceeded somewhat too rapidly at certain places in my articles published in this Journal several years ago.

DEFINITIONS AND NOTATION.

1. The six possible permutations of the three letters a, b, c are the following:

$$\begin{matrix} a & b & c \\ a & c & b \\ b & a & c \\ b & c & a \\ c & a & b \\ c & b & a \end{matrix}$$

All of these may be obtained from any one of them, by replacing certain letters by others: *e. g.* the second is obtained from the first by replacing b by c and c by b. This operation is called a *substitution*, and it is denoted by bc; hence the substitutions are operations, while the permutations are results. The substitutions by means of which the given permutations are obtained from the

first are, in order, bc, ab, abc, acb, ac. If these substitutions are applied to *any* one of the given six permutations all the others are obtained. It is convenient to say that a permutation is obtained from itself by the substitution 1 or identity. If we add this substitution to the preceding set we may say that each of the given permutations may be obtained from any one of them by means of one of the following six substitutions:

$$1,\ abc,\ acb,\ ab,\ ac,\ bc.$$

If we apply a given substitution (s) to a given permutation and then apply the same substitution to the resulting permutation we obtain the same result as we would have obtained by applying some other substitution to the original permutation. This substitution is called the square of the given substitution and it is denoted by s^2. *E. g.* if $s=bc$ then $s^2=1$; for if we apply bc twice we obtain the original permutation; and if $s=abc$* then $s^2=acb$, etc. In general, if we apply a substitution (s) n times in succession the result is the same as it would have been if we had applied a certain substitution s^n a single time. The smallest positive value of n that satisfies the relation $s^n=1$ is said to be the *order* of s. Hence we say that three (bc, ab, ac) of the given six substitutions are of order two, two (abc, acb) are of order three, while identity may be said to be of order 0.

If we apply two different substitutions successively, we obtain the same permutation as we would have obtained by applying some substitution a single time. This single substitution which is equivalent to the two substitutions applied successively is said to be their *product*. *E. g.* if we first apply ab and then ac we obtain the same result as if we had applied abc. Hence we say that $ab.ac=abc$. It may be observed that $ac.ab=acb$; *i. e.* the product of two substitutions need not be independent of their order, or the multiplication of substitutions is not always commutative.

Since it is very important that the reader should be able to multiply rapidly and accurately, each of the following products should be verified by the beginner.

$abc.acb=1$	$acb.abc=1$	$ab\ abc=ac$	$ac.abc=bc$	$bc.abc=ab$
$abc.abc=acb$	$acb.acb=abc$	$ab\ acb=bc$	$ac.acb=ab$	$bc.acb=ac$
$abc.ab=bc$	$acb.ab=ac$	$ab.ab=1$	$ac.ab=acb$	$bc.ab=abc$
$abc.ac=ab$	$acb.ac=bc$	$ab.ac=abc$	$ac.ac=1$	$bc.ac=acb$
$abc.bc=ac$	$acb\ bc=ab$	$ab.bc=acb$	$ac.bc=abc$	$bc.bc=1$

When a set of g different substitutions contains all the substitutions which may be obtained by multiplying any two of them or by squaring any one of them

***In performing the operation *abc.abc*, *i. e.* in multiplying *abc* into *abc*, we may say: In the first substitution *a* is replaced by *b* and in the second *b* is replaced by *c*, therefore *a* is replaced by *c* in the product; in the first substitution *c* is replaced by *a* and in the second *a* is replaced by *b*, therefore *c* is replaced by *b* in the product; in the first substitution *b* is replaced by *c* and in the second *c* is replaced by *a*, therefore *b* is replaced by *a* in the product. Since *a* is the first letter this completes the cycle and the given product is *acb*. It is to be observed that we take the letters in order; *e. g.* after finding that *a* is replaced by *c* in the product we next inquired by what *c* is replaced in the first substitution.**

the set is called a *substitution group* of order g. The number of different elements or letters that occur in all of the substitutions of the group is said to be the *degree* of the group. Hence the given six substitutions constitute a substitution group of order 6 and of degree 3. When a group is contained in a larger group it is said to be a *subgroup* of the larger group; *e. g.* the group of order 3 and degree 3 whose substitutions are 1, abc, acb is a subgroup of the given group of order 6. This group of order 6 contains four other subgroups, three of order 2, and one of order 1. It may be observed that the subgroup, identity, occurs in every group.

The substitution abc means that a is replaced by b, and then b by c, and finally c by a. If we suppose that these three letters are placed in the given order on the circumference of a circle at intervals of 120° the given substitution is equivalent to a positive rotation of this circle through 120° degrees. Hence such a substitution is called a cycle or a circular substitution. It is evident that the given notation is not unique, for $abc=bca=cab$. In general, if a circular substitution contains n elements it may be written in n ways. This indefiniteness is generally avoided by beginning with the first letter of the alphabet that occurs in the substitution. If this is done the notation becomes unique.

Any substitution whatever is the operation by means of which we may derive a particular permutation from a given arrangement of the elements involved in the substitution, and every rearrangement of the elements of a given permutation leads to a substitution in those elements. Hence we observe that any substitution consists either of a single cycle or of a series of cycles such that no two of them have a common element: *e. g.* the permutation $abcdefghi$ is obtained from the permutation $cabedifgh$ by means of the substitution $abc.de.fghi$, the periods being used to separate the complete cycles. Since the operations indicated by the different cycles may be performed independently of each other and in any order the given periods may also be interpreted as indicating multiplication.

According to the given notation *any series of letters or elements may be regarded as a substitution provided no letter occurs more than once in the series, and these letters are either not separated by any marks or they are divided into sets of two or more by means of periods.*

Hence there are two methods by means of which we can obtain all the possible substitutions that can be formed with a given number (n) of letters. By the first method we write down all the possible permutations of these n letters and find the substitutions by means of which we can obtain all the $n!$ permutations from any given one of them. By the second method we write down all the possible different substitutions that actually involve the n letters, then those that involve any combination of $n-1$, $n-2$, ... 3, 2 of them. The sum of these will, of course, be $n!$

The beginner would do well if he would find the twenty-four possible substitutions whose degree does not exceed four by means of each of these two methods. It may be remarked that there are just $(n-1)!$ circular substitutions that contain n given letters.